

Manual de Políticas de Seguridad y Uso de Recursos de Trabajo


Fecha de Actualización:
12 abril 2019

Elaborado por:  DATASOLUTIONS Ing. Anamaría Martínez Consultor	Revisado por:  Ma. Fernanda García Talento Humano	Aprobado por:  Presidente Ejecutivo José Vicente Ortega
--	---	---

 DATASOLUTIONS	MANUAL DE POLÍTICAS DE SEGURIDAD INFORMÁTICA Y USO DE RECURSOS DE TRABAJO	Fecha: Abril.2019
	MNP-SIURT	Versión: 01

Índice

1.	Generalidades	3
2.	Objetivos	3
3.	Estrategia Integral de Manejo de Seguridad Informática	3
4.	Instalaciones de los Equipos de Cómputo.	5
5.	Funcionamiento de los Equipos de Cómputo.....	5
6.	Responsabilidades Personales	6
7.	Identificadores de Usuario y Contraseñas	6
8.	Salida de Información	7
9.	Uso Apropiado de los Recursos	8
10.	Software.....	8
11.	Recursos de Red	9
12.	Conectividad a Internet	9
13.	Políticas de Monitoreo de Recursos Electrónicos e Informáticos	10
14.	Políticas de Seguridad Física	10
15.	Políticas de Uso de Instalaciones	11

 DATA SOLUTIONS	MANUAL DE POLÍTICAS DE SEGURIDAD INFORMÁTICA Y USO DE RECURSOS DE TRABAJO	Fecha: Abril.2019
	MNP-SIURT	Versión: 01

1. Generalidades

La seguridad informática ha tomado gran auge, debido a las cambiantes condiciones y nuevas plataformas tecnológicas disponibles. La posibilidad de interconectarse a través de redes, ha abierto nuevos horizontes a las empresas para mejorar su productividad y poder explorar más allá de las fronteras nacionales, lo cual lógicamente ha traído consigo, la aparición de nuevas amenazas para los sistemas de información. Estos riesgos que se enfrentan han llevado a que se desarrolle un documento de directrices que orientan en el uso adecuado de estas destrezas tecnológicas y recomendaciones para obtener el mayor provecho de estas ventajas, y evitar el uso indebido de la mismas, lo cual puede ocasionar serios problemas a los bienes, servicios y operaciones de la empresa.

En este sentido, las políticas de seguridad informática definidas partiendo desde el análisis de los riesgos a los que se encuentra propensa, surgen como una herramienta organizacional para concienciar a los colaboradores de la organización sobre la importancia y sensibilidad de la información y servicios críticos que permiten a la empresa crecer y mantenerse competitiva.

2. Objetivos

- Planear, organizar, dirigir y controlar las actividades para mantener y garantizar la integridad física de los recursos informáticos, así como resguardar los activos de la empresa.
- Establecer un esquema de seguridad con perfecta claridad y transparencia.
- Compromiso de todo el personal de la empresa con el proceso de seguridad, agilizando la aplicación de los controles con dinamismo y armonía.


3. Estrategia Integral de Manejo de Seguridad Informática

Para garantizar una mayor operatividad y continuidad de la infraestructura informática se debe tomar en cuenta una estrategia integral que considere todos los procesos técnicos, operativos y administrativos que se deben desarrollar y ejecutar para cumplir el objetivo. Para tal efecto se deben tomar en cuenta los siguientes criterios:

3.1. Prevención. La ejecución de un programa exhaustivo, integral y completo de mantenimiento preventivo, orientado a disminuir significativamente el índice de contingencias. Las actividades ejecutar para asegurar la prevención son:

- Limpieza externa de hardware y sus periféricos. ☐
- Limpieza interna de hardware y sus partes y piezas. ☐
- Preventivo de software. ☐
- Correctivo de software. ☐
- Elaboración de Informes: 1. Informe catastral cada vez que se efectúa una actividad de mantenimiento, 2. Reporte de actividades y 3. Informe de apoyo.
- Actividades relacionadas: 1. Revisión de tomas eléctricas y puntos de red, 2. Planificación anticipada de cada actividad, 3. Control de políticas de usuario y operatividad del equipo y 4. Etiquetado de los equipos. ☐
- Todos los puntos anteriores deberán cumplirse al momento de realizar los mantenimientos de equipos.
- Se deberá crear un cronograma de mantenimiento preventivo de equipos.

3.2. Escalabilidad.

 DATASOLUTIONS	MANUAL DE POLÍTICAS DE SEGURIDAD INFORMÁTICA Y USO DE RECURSOS DE TRABAJO	Fecha: Abril.2019
	MNP-SIURT	Versión: 01

- 3.2.1 Disponer de un equipo técnico con la adecuada coordinación para dar apoyo y soporte escalable, ya sea programado, por contingencia (servicio técnico) o por horas críticas. Las actividades a ejecutar para asegurar la escalabilidad son:
- Servicio de atención y organización por una Mesa de Servicio quien brindará soporte de primer nivel y da apoyo presencial al personal de Helpdesk en sitio. ☐
 - Cada técnico deberá generar una Orden de Servicio como respaldo y para elaboración de reportes mensuales. ☐
 - La Orden de Servicio es la aceptación de satisfacción del usuario del equipo. ☐
 - Los equipos operativos son aquellos que se encuentren en red, con la información y aplicativos que el usuario requiera para sus labores, y con los periféricos configurados correctamente, incluyendo impresoras ☐ locales o de red. ☐
 - Si el problema de un equipo no se puede resolver inmediatamente, debe dirigirse la solución del problema a personal técnico con conocimiento o a un proveedor externo.
 - Deben procesarse todas las garantías técnicas en la medida de lo posible.
- 3.2.2 En caso de contratar un servicio externo para la ejecución de la estrategia de escalabilidad, se deberá establecer expresamente,, entre las partes, los tiempos de respuestas y las multas que serán imputadas a la factura mensual en caso de incumplimiento de estos tiempos.
- 3.3. Simultaneidad.** Disponer de un equipo técnico que atienda las necesidades y requerimientos de manera simultánea y responder a varios eventos que se susciten a la vez. Las actividades ejecutar para asegurar la simultaneidad son:
- Restricciones y acceso a la navegación de acuerdo al perfil del usuario y requerido por ☐ Gerencia. ☐
 - Monitoreo del recurso de internet ☐
 - Monitoreo constante de total operatividad para el servicio Proxy-Firewall ☐
 - Creación, modificación y eliminación de cuentas de correo electrónico ☐
 - Monitoreo constante de total operatividad para el servicio de correo electrónico ☐
 - Administración del dominio y del directorio activo ☐
 - Control de las políticas de usuario. ☐
 - Revisión del log del sistema operativo ☐
 - Revisión de respaldos y tareas programadas
 - Soporte a la red
 - Configuración de la red inalámbrica
 - Detección de errores en la red Lan ☐
 - Configuración de switches y routers
- 3.4. Especialidad.** El equipo técnico deberá estar conformado por profesionales con las especialidades y capacitación requeridas para atender de forma eficiente y especializada cada tipo de equipamiento.
- 3.5. Procesos / Conocimiento.**
- El trabajo debe ser realizado considerando las mejores prácticas ITIL. Todos los servicios y actividades desarrolladas deber ser registradas y documentadas, conformando una base de conocimientos que permita, a través de su análisis, detectar patrones o tendencias que ayuden a tomar acciones preventivas al mismo tiempo que permitan solucionar con mayor velocidad las contingencias que ya hayan sido previamente solventadas. ☐

 DATA SOLUTIONS	MANUAL DE POLÍTICAS DE SEGURIDAD INFORMÁTICA Y USO DE RECURSOS DE TRABAJO	Fecha: Abril.2019
	MNP-SIURT	Versión: 01

- b. Los mantenimientos preventivos a los equipos deberán asegurar que los puertos USB estén bloqueados y no exista cambio alguno en el uso de los mismos.
- c. Deberá asegurarse la instalación y actualización de un antivirus en todos los equipos de la empresa.

3.6. Capacitación. El conocimiento adquirido debe documentarse con políticas de usuario y capacitaciones puntuales que permitan utilizar de forma correcta los equipos y auto-gestionar problemas técnicos menores. □

4. Instalaciones de los Equipos de Cómputo.


La instalación del equipo de cómputo, quedará sujeta a los siguientes lineamientos:

- 4.1. Los equipos para uso interno se instalarán en lugares adecuados, lejos del polvo y tráfico de personas.
- 4.2. Se deberá contar con un croquis actualizado de las instalaciones eléctricas y de comunicaciones de los equipos de cómputo en red. Actualmente se cuenta con el siguiente croquis:



- 4.3. Las instalaciones eléctricas y de comunicaciones estarán de preferencia fijas o en su defecto resguardadas del paso de personas o máquinas, y libres de cualquier interferencia eléctrica o magnética.
- 4.4. Las instalaciones se apegarán estrictamente a los requerimientos de los equipos, cuidando las especificaciones del cableado y de los circuitos de protección necesarios. En ningún caso se permitirán instalaciones improvisadas o sobrecargadas.

5. Funcionamiento de los Equipos de Cómputo.

	MANUAL DE POLÍTICAS DE SEGURIDAD INFORMÁTICA Y USO DE RECURSOS DE TRABAJO	Fecha: Abril.2019
	MNP-SIURT	Versión: 01


- 5.1 Es obligación del Jefe Administrativo Financiero vigilar que el equipo de cómputo se use bajo las condiciones especificadas por el proveedor y de acuerdo a las funciones del área a la que se asigne.
- 5.2 Los colaboradores de la empresa al usar el equipo de cómputo, se abstendrán de consumir alimentos, fumar o realizar actos que perjudiquen el funcionamiento del mismo o deterioren la información almacenada en medios magnéticos, ópticos, o medios de almacenamiento removibles de última generación.
- 5.3 Mantener claves de acceso que permitan el uso solamente al personal autorizado para ello.
- 5.4 Verificar la información que provenga de fuentes externas a fin de corroborar que esté libre de cualquier agente contaminante o perjudicial para el funcionamiento de los equipos.
- 5.5 Mantener pólizas de seguros de los recursos informáticos en funcionamiento.
- 5.6 En ningún caso se autorizará la utilización de dispositivos ajenos a los procesos informáticos del área. Por consiguiente, se prohíbe el ingreso y/o instalación de hardware y software particular, es decir que no sea propiedad de Datasolutions, excepto en casos emergentes que el Jefe Administrativo Financiero autorice.
- 5.7 Todas los equipos de computación deberán tener instalado el antivirus aprobado por el Gerente General, para proteger el equipo de cualquier infección.

6. Responsabilidades Personales

- 6.1 Los usuarios son responsables de toda actividad relacionada con el uso de su acceso autorizado.
- 6.2 Proteger, en la medida de sus posibilidades, los datos de carácter personal a los que tienen acceso, contra revelaciones no autorizadas o accidentales, modificación, destrucción o mal uso, cualquiera que sea el soporte en que se encuentren contenidos los datos.
- 6.3 Disminuir la cantidad de correos basuras.
- 6.4 Mantener las soluciones activadas y actualizadas.
- 6.5 Verificar los archivos adjuntos de mensajes sospechosos y evitar su descarga en caso de duda.
- 6.6 Cualquier incumplimiento de los literal 6.1. al 6.5. será considerado una falta grave de acuerdo al reglamento interno por lo cual se emitirá los files o multas la especifique en dicho documento.

7. Identificadores de Usuario y Contraseñas


- 7.1. Todos los usuarios con acceso a un sistema informático o a una red informática, dispondrán de una única autorización de acceso compuesta de identificador de usuario y contraseña.

 DATASOLUTIONS	MANUAL DE POLÍTICAS DE SEGURIDAD INFORMÁTICA Y USO DE RECURSOS DE TRABAJO	Fecha: Abril.2019
	MNP-SIURT	Versión: 01

- 7.2. Ningún usuario recibirá un identificador de acceso a la red de comunicaciones, recursos informáticos o aplicaciones hasta que no acepte formalmente la política de seguridad vigente.
- 7.3. Los usuarios tendrán acceso autorizado únicamente a aquellos datos y recursos que precisen para el desarrollo de sus funciones, conforme a los criterios establecidos por el responsable de la información.
- 7.4. Los usuarios no deben revelar bajo ningún concepto su identificador y/o contraseña a otra persona ni mantenerla por escrito a la vista, ni al alcance de terceros.
- 7.5. Los usuarios no deben utilizar ningún acceso autorizado de otro usuario, aunque dispongan de la autorización del propietario.
- 7.6. Si un usuario tiene sospechas de que su acceso autorizado (identificador de usuario y contraseña) está siendo utilizado por otra persona, debe proceder al cambio de su contraseña e informar a su jefe inmediato y éste reportar al responsable de la administración de la red.
- 7.7. El usuario debe utilizar una contraseña compuesta por un mínimo de ocho caracteres constituida por una combinación de caracteres alfabéticos, numéricos y especiales.
- 7.8. La contraseña no debe hacer referencia a ningún concepto, objeto o idea reconocible. Por tanto, se debe evitar utilizar en las contraseñas fechas significativas, días de la semana, meses del año, nombres de personas, teléfonos.
- 7.9. En caso que el sistema no lo solicite automáticamente, el usuario debe cambiar la contraseña provisional asignada la primera vez que realiza un acceso válido al sistema.
- 7.10. En el caso que el sistema no lo solicite automáticamente, el usuario debe cambiar su contraseña como mínimo una vez cada 30 días. En caso contrario, se le podrá denegar el acceso y se deberá contactar con el jefe inmediato para solicitar al administrador de la red una nueva clave.

8. Salida de Información

- 8.1 Toda salida de información (en soportes informáticos o por correo electrónico) sólo podrá ser realizada por personal autorizado y será necesaria la autorización formal del responsable del área del que proviene.
- 8.2 Los puertos USB de las computadoras de la compañía deberán estar deshabilitados para reducir la transferencia de información de propiedad intelectual de Datasolutions y/o información confidencial de sus clientes, esto se refiere a que el personal de Datasolutions no podrá hacer uso de equipo electrónico (Teléfonos Celulares, Tablets, Laptops, Cámaras Fotográficas y de Video) en áreas operativas del centro de acopio, con el objetivo de salvaguardar la integridad de la información y su difusión o publicación en medios públicos o privados atentando contra la confidencialidad y la imagen de sus clientes.

 DATA SOLUTIONS	MANUAL DE POLÍTICAS DE SEGURIDAD INFORMÁTICA Y USO DE RECURSOS DE TRABAJO	Fecha: Abril.2019
	MNP-SIURT	Versión: 01

9. Uso Apropriado de los Recursos

9.1 Los recursos informáticos, datos, software, red corporativa y sistemas de comunicación electrónica están disponibles exclusivamente para cumplir las obligaciones y propósito de la operatividad para la que fueron diseñados e implantados. Todo el personal usuario de dichos recursos debe saber que no tiene el derecho de confidencialidad en su uso.

Se encuentra terminantemente prohibido:

9.2 El uso de estos recursos para actividades no relacionadas con el propósito del negocio, o bien con la extralimitación en su uso.

9.3 Introducir en los sistemas de información o la red corporativa contenidos obscenos, amenazadores, inmorales u ofensivos.

9.4 Introducir voluntariamente programas, virus, macros, controles ActiveX o cualquier otro dispositivo lógico o secuencia de caracteres que causen o sean susceptibles de causar cualquier tipo de alteración o daño en los recursos informáticos. El personal tendrá la obligación de utilizar los programas antivirus y sus actualizaciones para prevenir la entrada en los sistemas de cualquier elemento destinado a destruir o corromper los datos informáticos.

9.5 Intentar destruir, alterar, inutilizar o cualquier otra forma de dañar los datos, programas o documentos electrónicos.

9.6 Albergar datos de carácter personal en las unidades locales de disco de los computadores de trabajo.

9.7 Cualquier documento introducido en la red corporativa o en el puesto de trabajo del usuario a través de soportes automatizados, internet, correo electrónico o cualquier otro medio, deberá cumplir los requisitos establecidos en estas normas y, en especial, las referidas a propiedad intelectual y control de virus.

9.8 La descarga de músicas en los equipos, la utilización de la clave de wifi en equipos telefónicos, navegación en redes sociales, imágenes, músicas y archivos que no correspondan estrictamente para uso de trabajo.


10. Software

10.1 En las computadoras sólo debe existir archivos de Microsoft, sistema EDC y Windream para su uso durante las horas de trabajo; y el Jefe Administrativo Financiero asegurará la existencia de las licencias de dichos programas.

10.2 Todo el personal que accede a los sistemas de información de la empresa debe utilizar únicamente las versiones de software facilitadas y siguiendo sus normas de utilización.

10.3 Todo el personal tiene prohibido instalar copias ilegales de cualquier programa, incluidos los estandarizados.

10.4 También tiene prohibido borrar cualquiera de los programas instalados legalmente.

 DATA SOLUTIONS	MANUAL DE POLÍTICAS DE SEGURIDAD INFORMÁTICA Y USO DE RECURSOS DE TRABAJO	Fecha: Abril.2019
	MNP-SIURT	Versión: 01

11. Recursos de Red

De forma rigurosa, **ninguna persona debe:**

- 11.1 Conectar a recursos informáticos cualquier tipo de equipo de comunicaciones (ej. módem) que posibilite la conexión a la red corporativa.
- 11.2 Conectarse a la red corporativa a través de otros medios que no sean los definidos.
- 11.3 Intentar obtener otros derechos o accesos distintos a aquellos que les hayan sido asignados.
- 11.4 Intentar acceder a áreas restringidas de los sistemas de información o de la red corporativa.
- 11.5 Intentar distorsionar o falsear los registros "log" de los sistemas de información.
- 11.6 Intentar descifrar las claves, sistemas o algoritmos de cifrado y cualquier otro elemento de seguridad.
- 11.7 Poseer, desarrollar o ejecutar programas que pudieran interferir sobre el trabajo de otros usuarios, ni dañar o alterar los recursos informáticos.

12. Conectividad a Internet

- 12.1 La autorización de acceso a internet se concede exclusivamente para actividades de trabajo. Todos los colaboradores de la empresa tienen las mismas responsabilidades en cuanto al uso de Internet.
- 12.2 El acceso a internet se restringe exclusivamente a través de la red establecida para ello, es decir, por medio del sistema de seguridad con cortafuegos incorporado en la misma. No está permitido acceder a internet llamando directamente a un proveedor de servicio de acceso y usando un navegador, o con otras herramientas de internet conectándose con un módem.
- 12.3 Internet es una herramienta de trabajo. Todas las actividades en internet deben estar en relación con tareas y actividades del trabajo desempeñado.
- 12.4 Sólo puede haber transferencia de datos de o a internet en conexión con actividades propias del trabajo desempeñado.
- 12.5 En caso de tener que producirse una transmisión de datos importante, confidencial o relevante, sólo se podrán transmitir en forma encriptada.
- 12.6 El Jefe Administrativo Financiero asegurará el cambio de la clave wi-fi mínimo 2 veces al año.

 DATA SOLUTIONS	MANUAL DE POLÍTICAS DE SEGURIDAD INFORMÁTICA Y USO DE RECURSOS DE TRABAJO	Fecha: Abril.2019
	MNP-SIURT	Versión: 01

13. Políticas de Monitoreo de Recursos Electrónicos e Informáticos

13.1 Mantenimiento. Se debe planificar y ejecutar un exhaustivo Programa de Mantenimiento Preventivo Informático y Servicio Técnico en Sitio, que son actividades orientadas a dar operatividad y continuidad a la infraestructura de usuarios (PC, laptops e impresoras).

13.2 Backups.

13.2.1 Se debe realizar diariamente copias de seguridad de los datos informáticos con el fin de disponer de un medio para recuperarlos en caso de pérdida en la fuente original. Las copias de seguridad son útiles ante distintos eventos y usos:

- a. Recuperar los sistemas informáticos y los datos de una catástrofe informática, natural o ataque
- b. Restaurar una pequeña cantidad de archivos que pueden haberse eliminado accidentalmente, corrompido, infectado por un virus informático u otras causas
- c. Guardar información histórica de forma económica y permitiendo el traslado a ubicaciones distintas de la de los datos originales.

13.2.2 Se deberá tener preever la posibilidad del colapso del backup principal de información, por lo cual se deberá contar un con segundo medio de backup que apoye el aseguramiento de acceso a la información de la empresa.

13.3 Plan de Contingencias Informaticas. Se deberá crear un plan de contingencia informática que incluya al menos los siguientes puntos:


- a. Continuar con la operación del área con procedimientos informáticos alternos.
- b. Tener los respaldos de información en un lugar seguro, fuera del lugar en el que se encuentran los equipos.
- c. Tener el apoyo por medios magnéticos o en forma documental, de las operaciones necesarias para reconstruir los archivos dañados.
- d. Contar con un instructivo de operación para la detección de posibles fallas, para que toda acción correctiva se efectúe con la mínima degradación posible de los datos.
- e. Contar con un directorio del personal (interno o externo) de soporte, al cual se pueda recurrir en el momento en que se detecte cualquier anomalía.
- f. Ejecutar pruebas de la funcionalidad del plan.
- g. Mantener revisiones del plan a fin de efectuar las actualizaciones respectivas.

14. Políticas de Seguridad Física

14.1 Se deberá proveer a la compañía de seguridad física de personal experimentado, como guardias de seguridad.

14.2 El personal de seguridad deberá contar con un espacio físico (garita) en la que pueda observar en su mayoría las instalaciones de la empresa

14.3 Las funciones del personal de seguridad son las de proteger y auxiliar a los empleados y visitantes de la empresa, vigilar la propiedad tratando de evitar actos delictivos, localizar siniestros, actuar ante cualquier tipo de accidente o

 DATASOLUTIONS	MANUAL DE POLÍTICAS DE SEGURIDAD INFORMÁTICA Y USO DE RECURSOS DE TRABAJO	Fecha: Abril.2019
	MNP-SIURT	Versión: 01

emergencia en coordinación con los cuerpos y fuerzas de seguridad del estado, velar por la seguridad en actos y eventos y regular el tráfico en las instalaciones de la empresa.

14.4 Se deberá contar con una compañía de seguridad electrónica que brinde internamente el servicio de manejo de claves, alarma de seguridad, sensores de movimientos, humo, control de aperturas y cierres de Datasolutions para cualquier evento que se presente tomando en cuenta que si en caso de que ocurriera un incidente en días feriados deberá comunicarse a Presidente Ejecutivo, Jefe Administrativo Financiero y Jefe de Operaciones.

14.5 En caso de una emergencia, el Jefe de Operaciones, quien posee una copia de las llaves de compañía, será quien acuda al lugar de los hechos.

15. Políticas de Uso de Instalaciones

15.1. Garita.


- Los agentes de seguridad deberán ejercer la vigilancia y protección de bienes muebles e inmuebles, así como la protección de las personas que puedan encontrarse en los mismos.
- Los agentes de seguridad deberán efectuar controles de identidad en el acceso o en el interior de inmuebles determinados, sin que en ningún caso puedan retener la documentación personal una vez de haber sido anunciado a la extensión de Servicio al cliente y haber autorizado su ingreso.
- Los agentes de seguridad no están autorizados a recibir comisión de actos delictivos o infracciones en relación con el objeto de su protección.
- Los agentes de seguridad deberán permanecer en su garita en toda la jornada laboral, no podrán abandonar el puesto más de 3 minutos.
- Los agentes de seguridad será quienes avisen vía telefónica a las personas responsables de la compañía: Jefe de Operaciones, Jefe Financiero Administrativo y Presidente Ejecutivo.

15.2. Oficinas.

- Apagar las luces y equipos una vez haya finalizado el horario de la jornada laboral, para evitar cualquier catástrofe (Incendio).
- Dejar limpio y ordenado el lugar de trabajo.
- Dejar cerradas todas las puertas de cada área.
- Ninguna caja deberá quedar dentro de las oficinas al finalizar la jornada.

15.3. Bodegas.

- Apagar las luces y equipos una vez haya finalizado el horario de la jornada laboral, para evitar cualquier catástrofe (Incendio).
- Mantener limpio y ordenado el lugar de trabajo.
- El encargado de despacho deberá recibir las herramientas de trabajo una vez que haya culminado la jornada laboral.
- Una vez terminada la jornada laboral deberá realizar un chequeo general de cada pasillo que no exista ningún inconveniente.

 DATA SOLUTIONS	MANUAL DE POLÍTICAS DE SEGURIDAD INFORMÁTICA Y USO DE RECURSOS DE TRABAJO	Fecha: Abril.2019
	MNP-SIURT	Versión: 01

- e. Activar la alarma al momento de cerrar la compañía, para evitar cualquier incidente que pueda ocurrir, en casos que ocurra algún inconveniente podrán llamar a los responsables: Jefe de Operaciones, Jefe Financiero Administrativo y Presidente Ejecutivo.